

## UNITED STATES DISTRICT COURT

for the  
Northern District of New York

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case No. 1:19-MJ-769 (DJS)  
INFORMATION ASSOCIATED WITH AN ACCOUNT )  
THAT IS STORED AT PREMISES CONTROLLED BY )  
GOOGLE LLC )

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before May 10, 2021 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Daniel J. Stewart  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for        days (not to exceed 30) ☐ until, the facts justifying, the later specific date of       

Date and time issued: April 26, 2021

City and state: Albany, New York

  
Judge's signature  
Daniel J. Stewart, U.S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.: 1:19-MJ-769 (DJS)	Date and time warrant executed: 05/26/21 5:16 PM	Copy of warrant and inventory left with: Google LLC
--------------------------------	---	--

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

on 05/04/21, Google digitally returned search warrant information to the Google Law Enforcement Request System (LERS). The information was downloaded on 05/04/21.

The downloaded files returned were:

- 1) 5738971-20210504-1 (zip file)
- 2) SW Letter 5738971 (pdf)

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 05/05/21

  
 Executing officer's signature  
 Matthew Twobly FBI Special Agent  
 Printed name and title

**ATTACHMENT A**

***Property to Be Searched***

This warrant applies to information associated with the Google account [lifetimesweeps@gmail.com](mailto:lifetimesweeps@gmail.com) (the “Target Account”) that is stored at premises owned, maintained, controlled, and/or operated by Google LLC, a company that accepts service of legal process and is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B**

***Particular Things To Be Seized***

**I. Information To Be Disclosed By Google LLC (“Google” or “Provider”) To Facilitate Execution Of The Warrant**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A (the “Target Account”) for the time period **January 1, 2019 to present**:

- a. the contents of all emails and related transactional records for all Google services used by the subscriber/user of either of the Target Account (such as mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies); electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions),

Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

- b. The contents of all other data and related transactional records for all Google services used by any Target Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services including all services referenced in paragraph (a) above) including any information generated, modified, or stored by user(s) or Google in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);
- c. All Google records concerning the online search and browsing history associated with any Target Account or its users (such as information collected through tracking cookies);
- d. All records and other information concerning any document, or other computer file

created, stored, revised, or accessed in connection with the Target Account or by a Target Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

- e. All records regarding identification of any Target Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;
- f. All records pertaining to devices associated with any Target Account and software used to create and access the Target Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities (“IMEI”), Mobile Equipment Identifiers (“MEID”), Global Unique Identifiers (“GUID”), Electronic Serial Numbers (“ESN”), Android Device IDs, phone numbers, Media Access Control (“MAC”) addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s), including unique application

numbers and push notification tokens associated with the Account (including Apple Push Notifications (“APN”), Google Cloud Messaging (“GCM”), Microsoft Push Notification Service (“MPNS”), Windows Push Notification Service (“WNS”), Amazon Device Messaging (“ADM”), Firebase Cloud Messaging (“FCM”), and Baidu Cloud Push);

- g. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any Google account (including both current and historical accounts) ever linked to the Target Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (e.g., credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;
- h. All information held by Google related to the location and location history of the user(s) of the Target Account, including geographic locations associated with the Target Account (including those collected for non-Google based applications), IP addresses, Global Positioning System (“GPS”) information, and information pertaining to nearby devices, Wi-Fi access points, and cell towers;
- i. All records of communications between Google and any person regarding the Target Account, including contacts with support services and records of actions taken;
- j. Information about any complaint, alert, or other indication of malware, fraud, or

terms of service violation related to a Target Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Target Account or associated user(s) (but not including confidential communications with legal counsel).

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

## **II. Information To Be Seized By The Government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 912 (False Impersonation of an Officer), 1341 (Mail Fraud), 1343 (Wire Fraud) and 1349 (Conspiracy) for the account listed on Attachment A (the “Target Account”), described as follows:

- a. Evidence of schemes to defraud, including pre-payment frauds, financial frauds, romance frauds, and lottery frauds; the targeting of victims for such schemes; and the disposition of proceeds of such schemes;
- b. Evidence of schemes involving the impersonation of others, including federal prosecutors, businesspeople, government officials; the targeting of victims for such schemes; and the disposition of proceeds of such schemes;
- c. Documents or communications concerning purported lottery winnings, prize money, trust proceeds, inheritances, or other financial opportunities;
- d. Evidence concerning the identity and role of persons who (i) collaborated, conspired, or assisted (knowingly or unknowingly) with the commission of the crimes under investigation; or (ii) communicated with the Target Account about matters relating to the crimes under investigation, including records that help reveal



their whereabouts;

- e. Evidence indicating the state of mind (*e.g.*, intent, absence of mistake, or evidence indicating preparation or planning) of the user(s) of the Target Account related to the criminal activity under investigation;
- f. The identity of the person(s) who created and/or used the Target Account, including records that help reveal the whereabouts of such person(s);
- g. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of the account's access, use, and events relating to the crimes under investigation and the identity of the owner(s) of the account.

### **III. Government Procedures For Warrant Execution**

The United States government will conduct a search of the information produced by the Google and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Google that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.